(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 994 598 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.04.2000 Bulletin 2000/16

(51) Int. Cl.^{7}: H04L 9/00

(21) Application number: 98830601.5

(22) Date of filing: 12.10.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant:
STMicroelectronics S.r.l.
20041 Agrate Brianza (Milano) (IT)

(72) Inventors:
- Italia, fransceco
95125 Catania (IT)
- Fortuna, Luigi
96100 Siracusa (IT)
- Beritelli, Francesco
95127 Catania (IT)
- Di Cola, Eusebio
98100 Messina (IT)

(74) Representative:
Pellegri, Alberto et al
c/o Società Italiana Brevetti S.p.A.
Piazza Repubblica, 5
21100 Varese (IT)

(54) Cryptation system for packet switching networks based on digital chaotic models

(57) A cryptation system for information transmitted through packet switching networks including masking the digital information data by combining them at the transmitting station with digital data of a certain code of cryptation before transmitting the so encrypted data through the network and performing an inverse decrypting processing at the receiving station using the same code of encrypting, comprises generating at a transmitting station and at a receiving station, starting from a given pair of password codes or user key, a certain discrete chaotic model or map of said pair of codes or key, producing dynamically updated pairs of values of codes or keys every certain number of processing steps of said chaotic map, masking the data to be transmitted by way of a logic combination with said current dynamically updated keys at the transmitting station, demasking the data at the receiving station by way of a logic decomposition of said digital data from said current dynamically updated key returning the digital data to a clear condition.

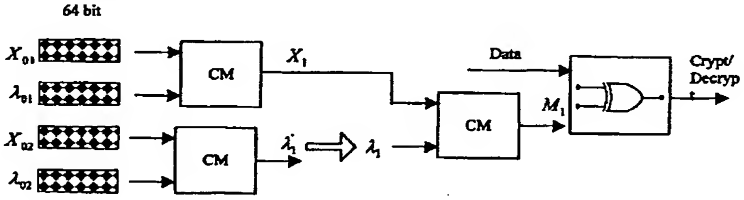

Fig. 3a Masking with chaotic key of second layer

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

FIELD OF THE INVENTION

[0001] The present invention relates to a method and relative system architecture for encrypting cryptation data transmitted on packet switching networks.

BACKGROUND OF THE INVENTION

[0002] The growing development of networks and broadband telecommunication services and among these of pay services and of the growing demand for increasingly high security standards of the privacy of the data transmitted have dictated a strong request for data encrypting systems and algorithms. Among the most important applications we may recall the encrypting video of transmission for *pay TV* services, of telephone conversations through mobile radio systems, of data transmitted on a telematic network (electronic signatures, telematic bank operations, telematic trading, and the like).

[0003] Typically, telecommunication networks supporting these services are broadband networks, whose success is due to new network technologies and, in particular, to the flexibility of communication protocols (for example X.25, IP, ATM) based on the so-called packet switching techniques.

[0004] The packet switching technique is based on the segmentation of the information to be transmitted in the form of packets of digital data of adequate length depending on the needs, to which address data (header) are associated in order for the information to reach destination. With these techniques of transmission, the band is occupied only in presence of an effective traffic of data to be transmitted and different communications of different types of traffic may co-exist on a unique carrier.

[0005] If on one hand the Internet Protocol (IP) is emerging as the platform network with greater diffusion prospectives, on the other hand the advent of new systems and broadband media (optical fibers and coaxial cables) represent a concrete premise for offering to the users a wealth of new services based on the ATM technique (Asynchronous Transform Mode). In the future, the combination of service platforms such as Internet with the ATM transport technique may also contribute to accelerate the diffusion of applications based on the ATM technique.

[0006] In this scenario, security is becoming a primary requirement for all operators of the sector because telematic services are on the increase (home banking, virtual shopping, electronic trading, etc.) and they require a high degree of privacy of information.

[0007] Fig. 1 shows the functional scheme of a secure communication system which highlights the presence of encrypting (CRYPT) and decrypting (CRYPT^{1}) blocks for data protection. The CRYPT block at the transmitter station encrypts the messages (*clear text*) commonly through a password function, so that only authorized persons can retrieve the original message. The output of the encrypting (encoding) process, called *ciphered text*, is decrypted (decoded) at the receiver station by way of an enciphering password.

[0008] It has been noticed that methodologies based on chaos theory may be useful in cryptation techniques. Potentially they are much more undecryptable than traditional cryptation techniques (DES, RSA, IDEA, MD5, etc.) presently used in packet switching networks.

[0009] A starting point for the creation of chaotic cryptation systems are the so-called chaotic models. These, regardless of the meaning and the problems related to their development, are recursive systems which, given certain initial values, indefinitely evolve in time in a complex and unpredictable manner.

[0010] The following table indicates some of the most common discrete chaotic models (also referred to as maps).

Table 1: Mian chaotic maps

Chaotic Map	Function
Logistic map	$X_{n+1} = aX_n(1-X_n)$
Henon map	$X_{n+1} = 1 - aX_n^2 + Y_n$ $Y_{n+1} = bX_n$
Logarithmic map	$X_{n+1} = \ln(a\|X_n\|)$
Squared map	$X_{n+1} = a - X_n^2$
Cubic map	$X_{n+1} = Y_n$ $Y_{n+1} = aY_n - Y_n^3 - bX_n$

[0011] Each chaotic series is characterized by the relative key, that is by the values of the initial state x(0) and of the control parameters (parameters *a* and *b*).

[0012] Generally, in order to encrypt the stream of digital data without increasing the amount of transmitted information, the most appropriate solution to protect the information is that of masking, as shown in the example of Fig. 2.

[0013] According to this approach, the transmitted data are masked by hiding the information signal within a more complex one, generated by a chaotic system, by simply adding the two types of data. During the reception phase, the opposite operation must be carried out, that is discriminating between the received data and the information to be locally reconstructed through a system identical to that used for the transmission.

[0014] The delicate problem of synchronization which is addressed herein, is independent from the choice of a particular chaotic map.

[0015] Reliability and the very high level of security are the main advantages of chaotic cryptography.

[0016] Starting from different parameters, it is impossible to obtain two identical series even if the starting parameters differ very little. This is an intrinsic characteristic of chaotic systems.

[0017] The following technical papers relate to the problem of cryptation systems for packet switching networks.

- [1] B. Schneier, "Applied cryptography - Protocols, Algorithms and Source Code in C, John Wiley & Sons, 1994.
- [2] D. R. Frey, Chaotic Digital Encoding: An Approach to Secure Communication, IEEE Trans Circuits Syst.-Part II, vol. 40, no. 10, pp. 660-666,1993.
- [3] M. J. Ogorzalek, Taming Chaos: Part I-Synchronization, IEEE Trans Circuits Syst.-Part I, vol. 40, no. 10, pp. 693-6699,1993.
- [4] G. Kolumb (n, M. P. Kennedy and L. O. Chua, The Role of Synchronization in Digital Communications Using Chaos-Part I: Fundamentals of Digital Communications, IEEE Trans Circuits Syst.-Part I, vol. 44, no. 10, pp. 927-936,1997.
- [5] F. Dachselt, K. Kelber and W. Schwarz, Chaotic Coding and Cryptoanalysis, Proceedings of ISCAS '97, pp. 1061-1064, 1997.
- [6] William Stallings, "IPv6: The New Internet Protocol", IEEE Communications Magazine, July 1996, pp. 96-108.

OBJECT AND SUMMARY OF THE INVENTION

[0018] The aim of the invention is to provide for a cryptography system based on digital chaotic models with enhanced security based on an encrypting/decrypting symmetric system, employing a key that is dynamically updated by the chaotic system.

[0019] According to a preferred embodiment of the invention, the dynamic key continuously processed by a certain model or digital chaotic map, used for encrypting/decrypting the information symmetrically at the transmitter and at the receiver, is generated through a multilevel architecture thus to provide for a scaleable degree of security, depending on the user's needs; a higher degree of security being obtained at the expense of an increment of the time taken for encrypting/decrypting.

[0020] The method of the invention, considers the organization of packets of crypted data with a header of data having a predefined and constant length, and with a payload of a variable length containing the crypted information.

[0021] The invention is defined in the independent claims 1 and 4, and particularly effective embodiments are defined in the claims 2, 3 and 5.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022]

Figure 1 is the scheme of a cryptation system for packet switching transmission networks.
Figure 2 is a scheme of cryptography based on a chaotic masking.
Figure 3a shows a cryptography scheme of the invention with a second level key.
Figure 3b shows the chaotic evolution of the state, referred to the scheme of Fig. 3a.
Figure 3c shows the chaotic evolution of the control parameter, referred to the scheme of Fig. 3a.
Figure 3d shows a cryptography scheme of the invention with a third level key.
Figure 4 shows the complete structure of a packet of crypted data.
Figure 5 is a detail of the header.
Figure 6 is a secure communication scheme for MPEG sequences transmitted on an ATM network.
Figure 7 shows the known structure of an MPEG-TS (a) packet and a detail of the 4 byte header of the MPEG-TS (b) packet.
Figure 8 shows a decoding system of MPEG sequences received through an ATM network.
Figure 9 shows the constitution of a corresponding crypted packet according to the present invention.
Figure 10 shows the architecture of the cryptography model according to the invention.
Figure 11 is a detail of the FUNC module of the architecture of Fig. 10.
Figure 12 shows the organization of the RAM memory of the cryptography module.

DESCRIPTION OF THE INVENTION

[0023] The key used for the masking sequence is composed by two elements or codes:

- State (64 bits)
- Control parameter (64 bits)

[0024] The combination of these two elements constitutes the key which permits to decrypt the crypted message or to encrypt a message.

[0025] The system of the invention is based on a symmetrical cryptography algorithm with a dynamic key of a chaotic type. In particular, the system dynamically updates both the State and the Control parameters of the chaotic series or map that is used for masking the information. Even, the laws of updating the initial State and Control parameters, or of the plurality of such elements in case of a scaleable multilevel scaleable implementation of the method of the invention, are of the chaotic type.

[0026] In practice, the user has at his disposal a double key, composed of four 64 bit codes, of which the first two represent the Control parameter and the initial State for which a chaotic series evolves generating a succession of Control parameters:

- c(0), c(1), c(2), ...
  the remaining two codes, represent instead the control parameter and the initial State from which a chaotic series evolves generating a succession of initial States:
- x(0), x(1), x(2), ...

[0027] By way of an example, according to the scheme of Fig. 3a, the above mentioned two successions may be obtained in the following manner.

[0028] Initially, the chaotic function is applied to the first key, formed by the two codes X_{01} λ_{01}, thus obtaining the

State parameter X_1. The same chaotic function is applied to the second key, formed by the two codes X_{02} λ_{02}, thus obtaining the Control parameter $\lambda_1^{'}$. However, the latter will range between 0 and 1 and in order to assure that the Control parameter is between 3.5 and 4 will be sufficient to apply a function capable to shift it within this interval. A very simple function that performs such a shift is:

$$\lambda_1 = \lambda_1^{'} \; OR \; (\mathrm{D400\ 0000\ 0000\ 0000})\mathrm{H}$$

[0029] The masking value M_1 may be derived by applying the chaotic function to λ_1 *and* X_1.

[0030] In order to encrypt or decrypt the datum D_1 it is sufficient to carry out an EXOR function or any other type of logic combination between the so generated masking value M_1 and the datum D_1.

[0031] The successive masking value M_2 with which encrypt the datum D_2 is obtained by applying the chaotic function to λ_1 *and to* M_1; similarly M_3 will be obtained by applying the chaotic function to λ_1 and to M_2, and so forth.

[0032] When there is a need to evolve the map related to the control parameter, the chaotic function is applied to X_1 and λ_{01}, thus obtaining the state X_2; the same chaotic function is applied to $\lambda_1^{'}$ and λ_{02}, thus obtaining the control parameter $\lambda_2^{'}$ which may be shifted to the appropriate range by the single function

$$\lambda_2 = \lambda_2^{'} \; OR \; (\mathrm{D400\ 0000\ 0000\ 0000})\mathrm{H}.$$

[0033] A new masking value will be defined by applying the chaotic function to λ_2 *and* X_2.

[0034] It should be noted that the masking value is comprised between 0 and 1, therefore its 64 bit corresponding value will have the two most significant bits at 0 (this originates from placing by way of example $2^{62} = 1$). This could impede the masking of the two most significant bits of the datum to be crypted. The problem may be solved simply by copying (only for the masking phase) the two bits of weight 60 and 61 into the two most significant bits or in any case giving to these two bits (63, 64) any casual values.

SCALEABLE MULTILEVEL CHAOTIC KEY

[0035] It is possible to further generalize the algorithm of the invention for generating the keys that govern the dynamic masking of the information, by implementing a scaleable multilevel key generation architecture.

[0036] As depicted in Fig. 3b, the initial State and the Control parameters of the n-th stage are generated in the preceding stage with a chaotic law. This has two advantages:

1) the system has a scaleable security degree;
2) the output masking sequence has an enhanced unpredictability.

[0037] Of course, with a multilevel structure, it will be necessary to account either for an increment of the processing time, in case of a sequential implementation of the entire multilevel architecture, or for an increment of the required silicon area in case of a parallel implementation of the multilevel architecture.

[0038] Hence, the selection of the degree of security may be conditioned in some cases by speed requisites of data processing of the particular application.

[0039] More in general, the scaleable multilevel architecture may be structured as a unique processing block receiving as input, besides the key of cryptation, also the desired security level for the specific application.

[0040] Naturally, the dynamic of the CM block output signals, which will be used in the successive stage, must be adapted to be appropriate as a Control parameter in the successive stage. In case of a logistic map, this adaptation may be done by implementing an OR between the CM block output which processes the map and the hexadecimal value D400 0000 0000 0000.

DEFINITION OF THE CRYPTED PACKET

[0041] According to a preferred embodiment of the invention, a new crypted packet (CRYPT packet) structure constituted of a header of data having a constant length and of a payload of variable length is defined as shown in the example of Fig. 4.

[0042] Naturally, the packet will include the packet header (indicated with a dark tone shading in the figure) according to the particular communication protocol being used.

[0043] The header of the crypted data packets contains a series of fields which are useful during the encrypting of the information. The data header includes a first packet identifying field (PID) and a second field (SID) that identifies the data stream to which the packet belongs (for those applications based on the transmission of a plurality of different streams). Moreover, in those cases wherein it is possible to structure the information in "messages", that is in groups of

CRYPT packets of a constant length, a third field (MID) identifying the message to which the packet belongs and a fourth field (CC) carrying information on the progressive number (continuity counter) of the packet within the message, may be also present.

[0044] In such a case, the crypting may be done at the message level, that is for each new message there is a change of key. Where the processing preceding the encrypting provides for already packeted data, the length of the header (HL) of the packeted data is indicated in order to prevent that such a header be encrypted. Finally, a field indicating the payload length of the crypted packet (PL) may be included for applications where it is necessary to account for a payload of variable length. Since the loss of a portion of a crypted packet signifies the loss of the entire packet, it is convenient to choose a PL value not excessively large. Of course, on the other hand, there is a need to guarantee a certain minimum length of the packet so that the ratio overhead header/payload be as small as possible.

[0045] Fig. 5 shows the organization of the data header according to an embodiment of the invention.

[0046] The data header of the crypted packet is subdivided into the following fields:

- PID (Packet IDentifier): is an identifier which permits to appropriately identify the packet as a CRYPT packet.
- SID (Stream IDentifier): is the unique identifier of the stream (i.e. a filmed sequence) to which the packet belongs. It implicitly permits to establish when should stop the encrypting of a certain stream and start the encrypting of another stream.
- MID (Message IDentifier): is the unique identifier of the message to which the packet belongs. It implicitly permits to establish when a change of key should be done.
- CC (Continuity Counter): indicates the number of the packet within the message. It permits, during the reception phase, to detect an eventual loss of packets because during the transmission it is incremented one unit at the time.
- SL (Security Level): indicates the chosen security level of protection of the information.
- HL (Header Length): indicates the length in bytes of the header of the packet of data header contained in the payload. For certain types of data, headerless data, its value will be 0.
- PL (Payload Length): indicates the length in bytes of the payload of the crypted packet. It serves to maintain the synchronism in case of a loss of crypted packets.

[0047] The peculiarities and advantages of the system of the invention may be summarized as follows:

1. The algorithm has a high level of security. The chaotic models, belonging to the class of polyalphabetical ciphers, ensure a higher degree of security than monoalphabetic ciphers (for example DES). Moreover, the dynamic change of key increases even further the level of security provided by the system of the invention. The law according to which the key is dynamically updated is of the chaotic type too and the frequency of updating may be chosen taking into consideration the characteristics of the particular application. Finally, to prevent cryptation of essential communication data and facilitate the use of the cryptation system, the masking is applied only to the data field (payload) of the packet. The HL field included in the header of the crypted packet permits a correct synchronization, preventing cryptation of the header portion of the packets.
2. According to a preferred embodiment, the level of security is scaleable. A multilevel architecture, by employing the same hardware, can readily adapt the level of security to the specific application requirements.
3. The algorithm exploits the intrinsic synchronism of the communication protocol based on the packet switched technique. During reception, by analyzing eventual discontinuities in the MID or CC fields, it is possible to trace back the number of the lost crypted packets.
4. The definition of the cryptography protocol provides for a certain flexibility also in the selection of the layer of application of the cryptography block.
5. The structure of the crypted packet is very flexible. It is capable to manage data streams of variable lengths with or without header.
6. The decrypting algorithm is independent of the particular type of information transmitted (audio, video, data) and of the eventual processing undergone by the messages (compression, etc.).

APPLICATION OF THE ALGORITHM OF THE INVENTION TO MPEG TRANSMISSION ON ATM NETWORKS

[0048] The application taken into consideration by way of example is that of a secure system of communication for MPEG video sequences transmitted on an ATM network. The encrypting/decrypting architecture of the invention may be integrated in a VLSI device of a functional hardware system, such as for example a "Set Top Box" for multimedia applications, as schematized in Fig. 6.

MPEG CODING

[0049] In terms of digital data, an MPEG video may be seen as a sequence of bits (bitstream). In particular, at the co-decoding level, that is at the coder output and at the decoder input, an MPEG film is delimited by sequence limiters; it always begins with a header, which contains essential coding information, such as for example: the frame size and the rate at which they are transmitted and the bit-rate, and terminates with a 32 bit end of sequence indicator.

[0050] The header is followed by a variable number of groups of frames, called GOP (Group Of Pictures); these provide for a random access to the pictures and represent the smallest entity that may be independently decoded. A GOP always begins with a header and terminates in correspondence of the header of the successive GOP or with the end of sequence indicator.

[0051] At transmission level, the MPEG bitstream is structured in MPEG packet Transport Streams (MPEG-TS) constituted of a 4 byte header and a data field of 184 bytes, according to the scheme of Fig. 7.

[0052] Typically, the header of a MPEG-TS packet has eight data fields containing: the synchronizing byte (SYNC_BYTE), the identifier of the stream to which it belongs (PID) and the continuity counter (CONTINUITY_COUNTER) which, being composed of only 4 bits, zeroes itself every sixteen MPEG-TS packets.

[0053] Fig. 8 shows a functional diagram of the case of a de-coder of MPEG sequences transmitted on an ATM network. The network interface reorders and reassembles the ATM packets received. In case of a simple uncrypted MPEG stream, it returns the transport level structured information, that is in packets of 188 bytes organized according to the MPEG-2 Transport Stream format (MPEG-TS) shown in Fig. 7.

[0054] The microprocessors μP return the different MPEG streams from the transport level to the coding level. Another microprocessor, not shown in the figure, finally carries out the MPEG decoding operations. In case of errors or loss of ATM packets, the ATM interface discards the entire MPEG-TS packet and thereafter the μP effect a further test discarding packets eventually received with errors.

[0055] By way of example of an application, the cryptography block of the invention may be inserted at the transport level, for imposing a unique de-crypting system for all the streams, reducing the costs, the size and the complexity of the relative hardware architecture.

[0056] The cryptography system introduces information data within the payload of the crypted packet and sets the values of the relative header, as illustrated in Fig. 9.

[0057] During a reception phase, the CRIPT^{1} block performs the inverse operation (decrypting), returning the data to a transport level format.

[0058] Due to the fact that at the transport level the MPEG-TS packets may be multiplexed and may belong to different data streams, it is necessary to store the State of the chaotic map of each stream.

[0059] Fig. 10 shows a hardware architecture for the cryptography model of the invention.

[0060] The system comprises an input buffer Buff.IN, that serves to store a certain number of data which must be crypted or decrypted, an output buffer, Buff.OUT, in which the data are stored after having been crypted or decrypted. There is also a processor unit, CU, that analyzes the data stored, and controls whether the data are crypted or not, etc., a FUNC module for generating the selected chaotic function, a RAM in which to store the values necessary to the crypting/decrypting operations, such as for example the present State and the key State for each channel, the security level to be used for each channel, etc., and finally, a module that performs the sum or the difference between the masking digital sequence and the data contained in the payload.

[0061] As shown in Fig. 11, the FUNC module may be composed essentially of basic cells executing the elementary operations, for example in the case of the chaotic function $X_{n+1} = aX_n(1 - X_n)$ that generates the logistic map, the FUNC module is composed of two multipliers, X, and a module, 1-, which executes the operation. "1 minus the value present at the input of the module".

[0062] The RAM includes an array of elementary memory cells organized in a way to form a 64 bit memory per each address. The required RAM capacity is calculated in function of the maximum security level and the maximum number of channels; for example:

Password or key	Security level	Registers per channel	Memory Capacity
2 x 64 bit	1	1	800 byte (100 channels) 400 byte (50 channels)
4 x 64 bit	2	3	2400 byte (100 channels) 1200 byte (50 channels)

(continued)

Password or key	Security level	Registers per channel	Memory Capacity
8 x 64 bit	3	7	5600 byte (100 channels) 2800 byte (50 channels)
16 x 64 bit	4	15	12000 byte (100 channels) 6000 byte (50 channels)

[0063] Beside the information inherent to the different States and to the current Keys relative to each Channel, the RAM contains data for allowing the CU to recognize the security level that must be used for each channel.

[0064] In the example, 4 bits are used to define the security level for each channel, if there are 100 channels, besides the processing data area a further data storage areas of about 56 bytes must be accounted for.

[0065] The CU module is programmable. When the *cfg* pin is activated (such as for example after a reset) the data acquisition will not be interpreted as data to be crypted or decrypted, instead they will be configuring data (for example, setting the security level for each channel, etc.).

COMPUTING ASPECTS

[0066] By way of example, the operations necessary to encrypt a whole PES packet in case a security level of up to level 2 and a logistic chaotic function are chosen, are reported in the following tables.

[0067] Let:

Xki	= the initial State relative to the k-th chaotic map of the i-th level;
Cki	= the Control parameter relative to the k-th chaotic map of the i-th layer;
A	= register of the present State of the chaotic map;
B	= register of the Control parameter of the chaotic function;
F	= the chaotic function output;
Lik	= register storing the relative output of the k-th chaotic map of the i-th layer;
C	= register storing the output of the chaotic function;
D	= register storing the datum to be crypted;
S	= register storing the result of the masking sum/subtraction.

STEP	OPERATION	NUMBER OF CYCLES
0	PES ACQUISITION	(188+16)*2
1	CALCULATION RAM ADDRESS CONTAINING THE NUMBER OF LEVELS OF THE CURRENT CHANNEL	MAX 10
2	READING N° OF LEVELS FROM THE RAM	2
3	PROCESSING THE DATUM RELATIVE TO THE N° OF LEVELS	4
4	READ X11 FROM RAM	2
5	X11 => A	1
6	READ C11 FROM RAM	2
7	C11 => B	1

8	STORE F IN RAM (L11)	2
9	READ X21 FROM RAM	2
10	x21 => A	1
11	READ C21 FROM RAM	2
12	C21 => B	1
13	STORE F IN RAM (L21); F => B	2
14	READ L11 FROM RAM	2
15	L11 => A	1
16	STORE F IN RAM (L12); F => C; DATUM => D	2
17	S => OUT (FIRST DATUM)	8*2
18	F => B	1
19	STORE F IN RAM (L12); F => C; DATUM => D	2
20	S => OUT (SECOND DATUM)	8*2
21	F => B	1
22	STORE F IN RAM (L12); F => C; DATUM => D	2
23	S => OUT (THIRD DATUM)	8*2
24	PES ACQUISITION	(188+16)*2
25	CALCULATION RAM ADDRESS CONTAINING THE NUMBER OF LEVELS OF THE CURRENT CHANNEL	MAX 10
26	READING N° OF LEVELS FROM THE RAM	2
27	PROCESSING THE DATUM RELATIVE TO THE N° OF LEVELS	4
28	READ X11 FROM RAM	2
29	x11 => A	1
30	READ C11 FROM RAM	2
31	c11 => B	1
32	STORE F IN RAM (L11)	2
33	READ X21 FROM RAM	2
34	x21 => A	1
35	READ C21 FROM RAM	2
36	C21 => B	1

37	STORE F IN RAM (L12); F => B	2
38	READ L11 FROM RAM	2
39	L11 => A	1
40	STORE F IN RAM (L12); F => C; DATUM => D	2
41	S => OUT (FIRST DATUM)	8*2
42	F => B	1
43	STORE F IN RAM (L12); F => C; DATUM => D	2
44	S => OUT (SECOND DATUM)	8*2
45	F => B	1
46	STORE F IN RAM (L12); F => C; DATUM => D	2
47	S =>OUT (THIRD DATUM)	8*2
	TOTAL	1758
	MAXIMUM TIME BETWEEN A PES PACKET AND THE FOLLOWING ONE	40.000

[0068] As it may be observed, the time requisites are satisfied because the total number of clock cycles required is less by an order of magnitude than the maximum allowed value (the processing time between a PES packet and the next is of 40,000 cycles). Since the major computing burden is for the acquisition of the PES packet, it may be easily verified that even the highest security levels (3 and 4) satisfy the above mentioned time constraints.

Claims

1. A cryptation system for information transmitted through packet switching networks including masking the digital information data by combining them at the transmitting station with digital data of a certain code of cryptation before transmitting the so encrypted data through the network and performing an inverse processing or decrypting at the receiving station using the same code of encrypting, characterized in that it comprises the following steps:

   generating at a transmitting station and at a receiving station, starting from a given pair of password codes or user key, a certain discrete chaotic model or map of said pair of codes or key, producing dynamically updated pairs of values of codes or key everys certain number of processing steps of said chaotic map;
   masking the data to be transmitted by way of a logic combination with said current dynamically updated keys at the transmitting station;
   demasking the data at the receiving station by way of a logic decomposition of said digital data from said current dynamically updated key returning the digital data to a clear condition.

2. The method according to claim 1, characterized in that a sequence of chaotically evolving masking data, corresponding to a dynamically updated input key according to a certain chaotic map, to be summed to the information data at the transmitting station and to be subtracted from the received data at the receiving station, is generated by a multilevel architecture system, a dynamically updated key output by a level representing the input key of a successive level and so forth until a last level outputting said masking data;

   an architectural level processing a dynamically updated by a preceding architectural level input key and outputting a dynamically updated key according to a certain discrete chaotic model or chaotic map independently chosen from a plurality of chaotic models for said two architectural levels.

3. The method according to claim 1 or 2,0 characterized in that a crypted data packet has a structure comprising header of a constant length and a payload of variable length wherein crypted information data are introduced;

   the header of the crypted packet having at least seven fields;

   - PID (Packet IDentifier): is an identifier which permits to appropriately identify the packet as a CRYPT packet.
   - SID (Stream IDentifier): is the unique identifier of the stream (i.e. a filmed sequence) to which the packet belongs. It implicitly permits to establish when should stop the encrypting of a certain stream and start the encrypting of another stream.
   - MID (Message IDentifier): is the unique identifier of the message to which the packet belongs. It implicitly permits to establish when a change of key should be done.
   - CC (Continuity Counter): indicates the number of the packet within the message. It permits, during the reception phase, to detect an eventual loss of packets because during the transmission it is incremented one unit at the time.
   - SL (Security Level): indicates the chosen security level of protection of the information.
   - HL (Header Length): indicates the length in bytes of the header of the packet of data header contained in the payload. For certain types of data, headerless data, its value will be 0.
   - PL (Payload Length): indicates the length in bytes of the payload of the crypted packet. It serves to maintain the synchronism in case of a loss of crypted packets.

4. A receiving/transmitting station of a packet switching network including a system for encrypting/decrypting information being transmitted and/or received by masking digital information data with data of a certain cryptography key, comprising an interface of connection to the network (INTERFACE ATM), a module of encrypting or decrypting (CRIPT$^{\pm 1}$) the data and one or more decoding and processing pipelines of received data (μP, MPEG^{-1}, ...), said module (CRIPT$^{\pm 1}$) comprising an input buffer (Buff.IN) storing a certain quantity of input data to be crypted or decrypted, an output buffer (Buff.OUT) storing the decrypted or crypted data, a control unit (CU), a RAM memory storing data necessary for the cryption/decryption operation and a module (±) summing or subtracting a sequence of said masking data to or from a sequence of information data to be crypted or decrypted, characterized in that it comprises

   a module (FUNC) generating a certain chaotic function, chosen among a plurality of selectable chaotic functions, starting from a pair of codes or passwords constituting a starting key read by said control unit (CU) and input to said processing module (FUNC);
   the pair of codes identifying a current state of evolution of said chaotic function as produced by said module (FUNC) being periodically updated in said RAM memory for each communication channel and constituting the current masking data of the transmitted information, which are dynamically updated every certain number of clock pulses of processing of said chaotic function.

5. The receiving-transmitting station according to claim 4, wherein the encryption/decryption architecture is multilevel and the level of security of the encrypting/decrypting processing is scaleable depending on the requisites of a specific application.

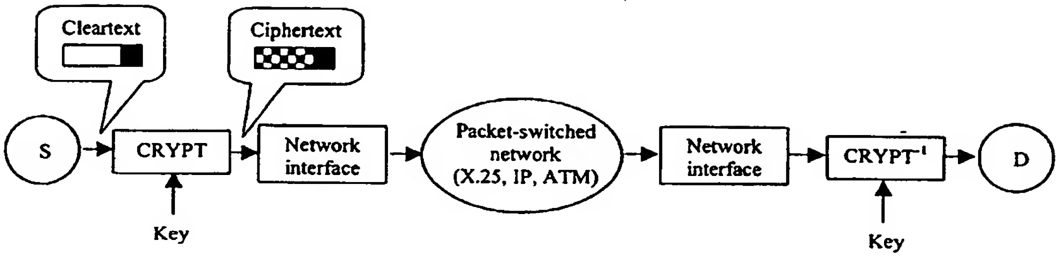
Cleartext
Ciphertext
S
CRYPT
Key
Network interface
Packet-switched network (X.25, IP, ATM)
Network interface
CRYPT⁻¹
Key
D

Fig. 1

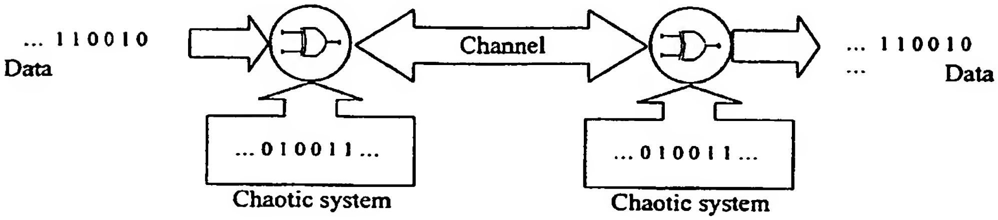
... 110010
Data
Channel
... 110010
...
Data
... 010011 ...
Chaotic system
... 010011 ...
Chaotic system

Fig. 2

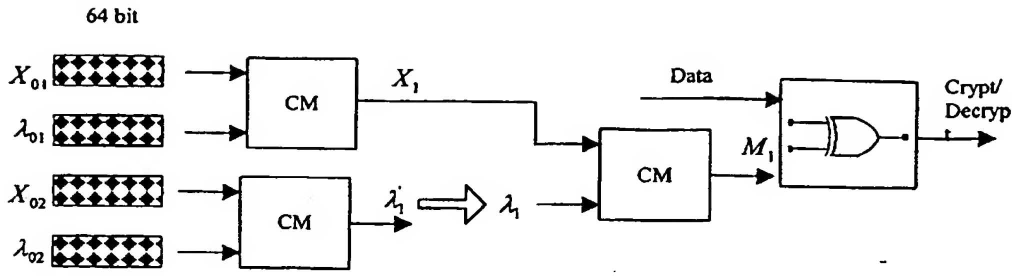

Fig. 3a Masking with chaotic key of second layer

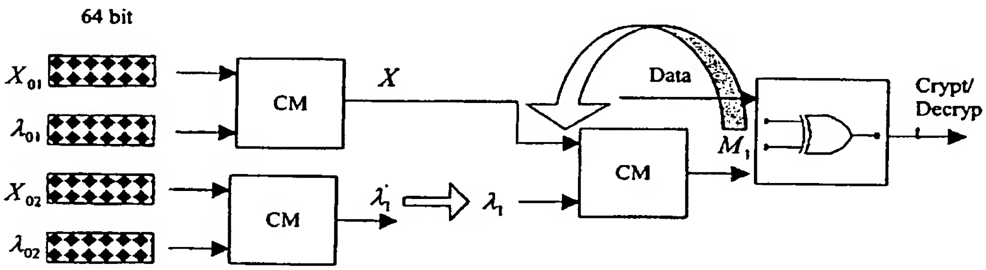

Fig. 3b State evolution

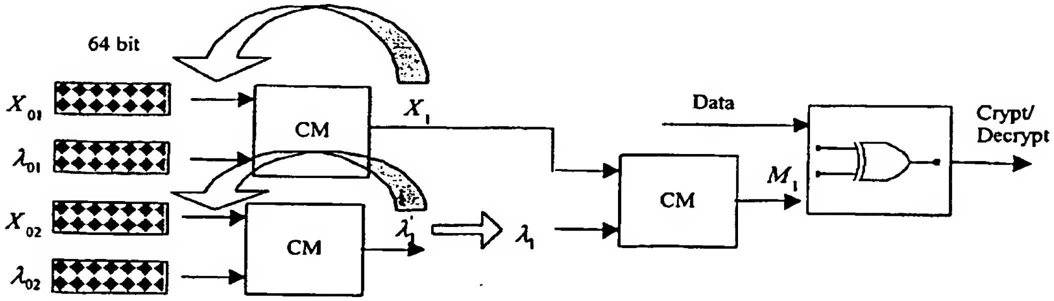

Fig. 3c Parameter control evolution

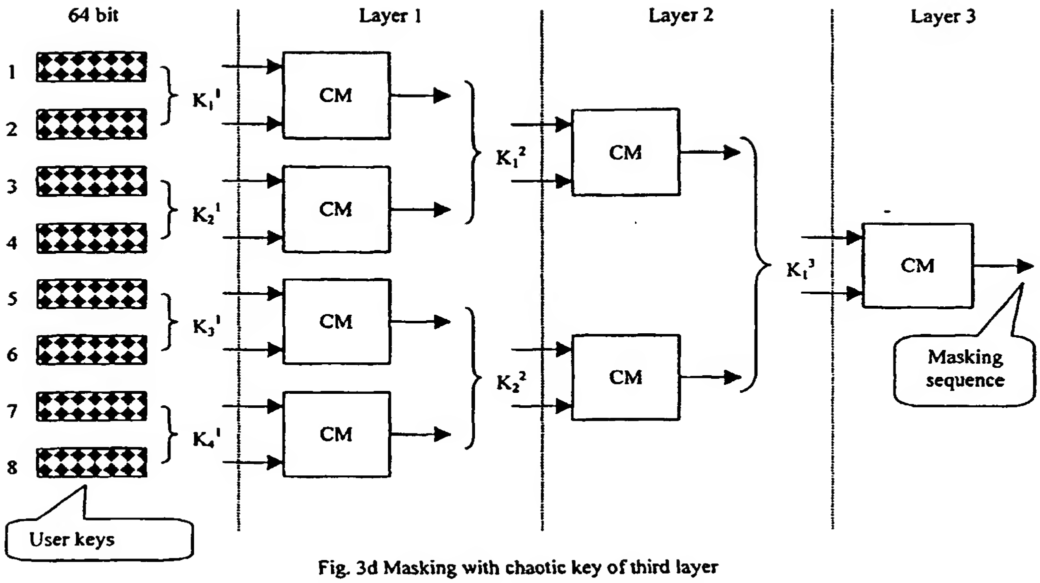

Fig. 3d Masking with chaotic key of third layer

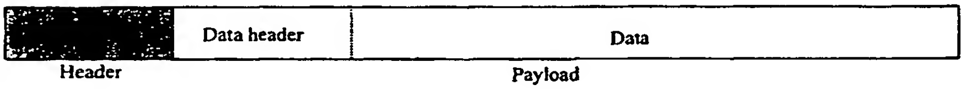

Fig. 4

PID (16 bit)	SID (16 bit)	MID (8 bit)	CC (12 bit)	SL (4 bit)	HL (8 bit)	PL (16 bit)

Fig. 5

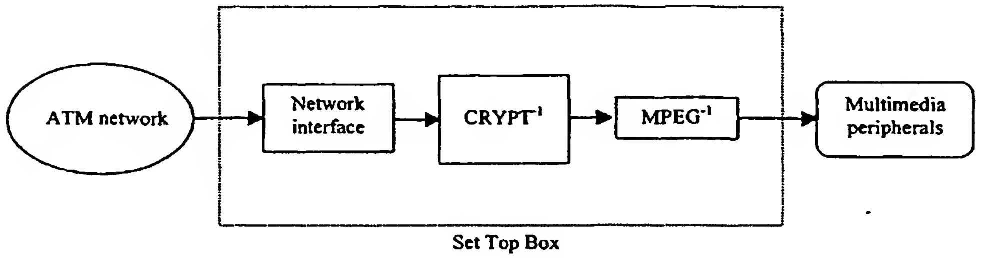

Fig. 6

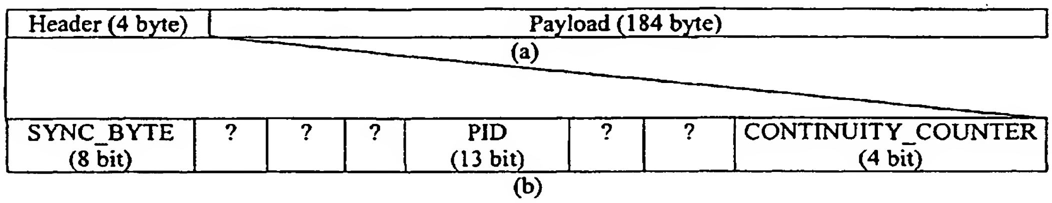

Fig. 7

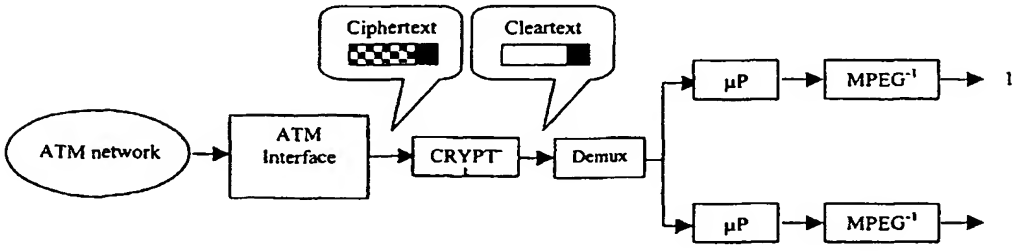

Fig. 8

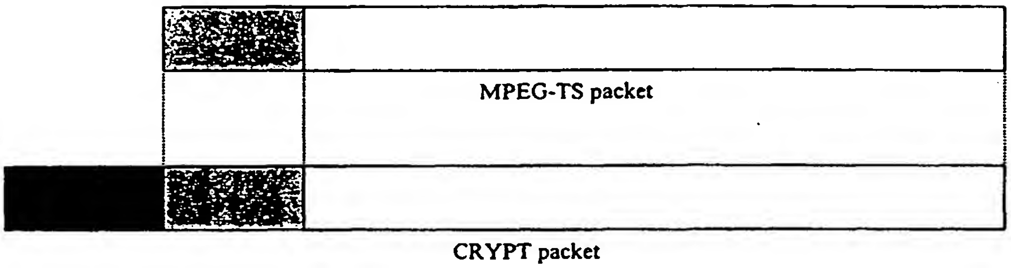

Fig. 9

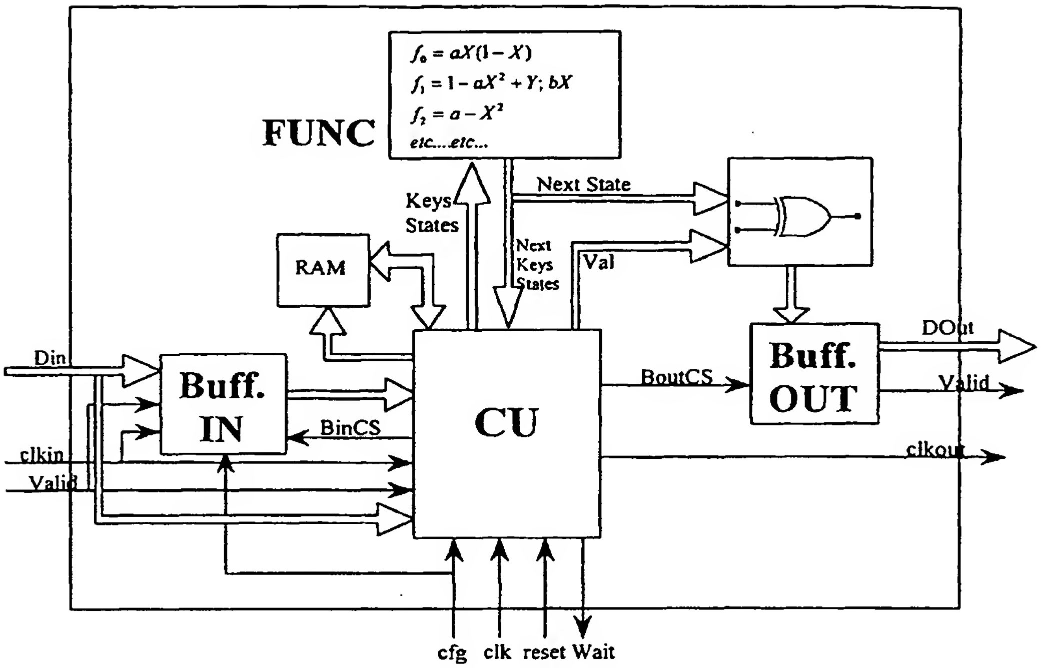
FUNC
$f_0 = aX(1-X)$
$f_1 = 1 - aX^2 + Y; bX$
$f_2 = a - X^2$
etc....etc...
Keys States
Next State
Next Keys States
Val
RAM
Din
Buff. IN
BinCS
CU
BoutCS
Buff. OUT
DOut
Valid
clkin
Valid
clkout
cfg
clk
reset
Wait

Fig. 10

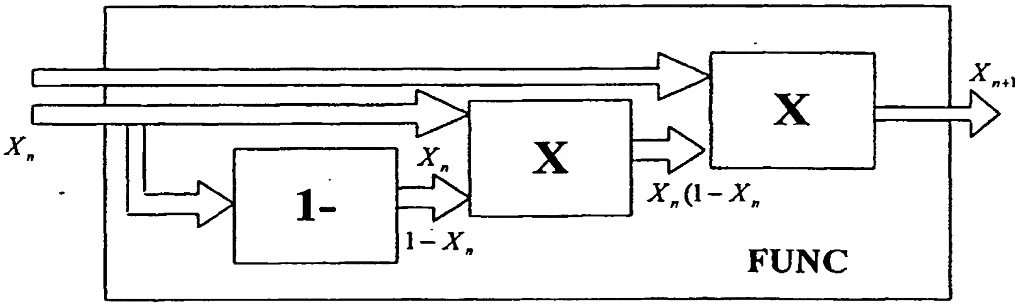
X_{n+1}
X_n
X
X
X_n
1-
$X_n(1-X_n$
$1-X_n$
FUNC

Fig. 11

Layer ch.1	Layer ch.2	Layer ch.3	Layer ch.4	....	Layer ch.16
Layer ch.17	Layer ch.18	Layer ch.19	Layer ch.20	....	Layer ch.32
Layer ch.33	Layer ch.34	Layer ch.35	Layer ch.36	....	Layer ch.48
Layer ch.49	Layer ch.50	Layer ch.51	Layer ch.52	....	Layer ch.64
Layer ch.65	Layer ch.66	Layer ch.67	Layer ch.68	....	Layer ch.80
Layer ch.81	Layer ch.82	Layer ch.83	Layer ch.84	....	Layer ch.96
Layer ch.97	Layer ch.98	Layer ch.99	Layer ch.100	....	

Fig. 12

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 83 0601

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	KOTULSKI Z ET AL: "Discrete chaotic cryptography" ANNALEN DER PHYSIK, 1997, BARTH, KÖLN (DE), vol. 6, no. 5, pages 381-394, XP002097239 ISSN 0003-3804 * page 382, line 16 - line 27 * * page 385, line 19 - line 30 * ---	1	H04L9/00
A	PATENT ABSTRACTS OF JAPAN vol. 098, no. 005, 30 April 1998 & JP 10 020783 A (METEOOLA SYST KK;AIRU:KK), 23 January 1998 * abstract * ---	1,4	
A	PATENT ABSTRACTS OF JAPAN vol. 098, no. 003, 27 February 1998 & JP 09 288565 A (TOSHIBA CORP;KODA TORU), 4 November 1997 * abstract * ---	1,4	
A	EP 0 467 239 A (HUGHES AIRCRAFT CO) 22 January 1992 * abstract; figure 4 * ----	1,4	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	19 March 1999	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 83 0601

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-03-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0467239 A	22-01-1992	US 5048086 A	10-09-1991
		DE 69118977 D	30-05-1996
		DE 69118977 T	19-09-1996
		JP 4250490 A	07-09-1992

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82